

ADELIC POINT GROUPS OF ELLIPTIC CURVES

ATHANASIOS ANGELAKIS AND PETER STEVENHAGEN

ABSTRACT. We show that for an elliptic curve E defined over a number field K , the group $E(\mathbf{A}_K)$ of points of E over the adèle ring \mathbf{A}_K of K is a topological group that can be analyzed in terms of the Galois representation associated to the torsion points of E . An explicit description of $E(\mathbf{A}_K)$ is given, and we prove that for K of degree n , ‘almost all’ elliptic curves over K have an adelic point group topologically isomorphic to

$$(\mathbf{R}/\mathbf{Z})^n \times \widehat{\mathbf{Z}}^n \times \prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}.$$

We also show that there exist infinitely many elliptic curves over K having a different adelic point group.

1. INTRODUCTION

Let K be a number field, and E an elliptic curve defined over K . An explicit model for E may be given by a short affine Weierstrass equation

$$(1) \quad E_{a,b} : y^2 = x^3 + ax + b$$

with integral coefficients $a, b \in K$ satisfying $\Delta_E = \Delta(a, b) = -16(4a^3 + 27b^2) \neq 0$. Given $E = E_{a,b}$, the set $E(K) \subset \mathbf{P}^2(K)$ of K -rational projective points naturally forms an abelian group with neutral element $O_E = (0 : 1 : 0)$. It is finitely generated by the *Mordell-Weil theorem*, and standard theory [9] shows that $E(K)$ can profitably be studied by viewing it as a subgroup of the \mathfrak{p} -adic point group $E(K_{\mathfrak{p}})$ of E over the completions $K_{\mathfrak{p}}$ at finite or infinite primes of K , or by mapping it at suitable primes \mathfrak{p} to the finite point group $\overline{E}(k_{\mathfrak{p}})$ of the reduced curve over the residue class field at \mathfrak{p} .

In this paper, we study the *adelic point group* of elliptic curves E/K , which we can define in view of Lemma 2.1 as the product

$$(2) \quad E(\mathbf{A}_K) = \prod_{\mathfrak{p} \leq \infty} E(K_{\mathfrak{p}})$$

of the point groups of E over *all* completions of K , both finite and infinite. The group $E(\mathbf{A}_K)$ is an uncountable abelian group that contains all \mathfrak{p} -adic point groups as subgroups, and naturally surjects to the point groups $\overline{E}(k_{\mathfrak{p}})$ at primes of good reduction. Unlike $E(K)$, which has no interesting topology, $E(\mathbf{A}_K)$ is in a natural way a compact topological group.

The behavior of the group $E(K)$ for fixed K and varying E still holds many mysteries. For the finite torsion subgroup $E(K)^{\text{tor}} \subset E(K)$, which, unlike $E(K)$ itself, is algorithmically well under control, we have bounds on its size in terms of

Date: March 27, 2017.

2010 *Mathematics Subject Classification.* Primary 11G05, 11G07; Secondary 11F80.

Key words and phrases. Elliptic curves, adelic points, Galois representation.

the degree of K (Merel's theorem, made effective by Parent), and we know that it is the trivial group for 'most' E over K . The rank of the free abelian group $E(K)/E(K)^{\text{tor}}$ is however not well understood. Among the latest progress is the work of Bhargava and Shankar [3] bounding its *average* value over $K = \mathbf{Q}$. If the rank itself remains bounded for fixed K and varying E is a question that is wide open, with new heuristics [6] now predicting that this should be the case for all K .

In view of the above, it may come as a surprise that the adelic point group $E(\mathbf{A}_K)$ not only admits a rather simple explicit description as a compact topological group, but that this description is also almost universal in the sense that most E over K give rise to the *same* adelic point group.

Theorem 1.1. *Let K be a number field of degree n . Then for almost all elliptic curves E/K , the adelic point group $E(\mathbf{A}_K)$ is topologically isomorphic to the universal group*

$$\mathcal{E}_n = (\mathbf{R}/\mathbf{Z})^n \times \widehat{\mathbf{Z}}^n \times \prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$$

associated to the degree n of K .

Remark 1.2. The notion of 'almost all' in Theorem 1.1 is the same as in [10], and is based on the counting of integral Weierstrass models $E_{a,b}$ given by (1). To define it, we fix a norm $\|\cdot\|$ on the real vector space $\mathbf{R} \otimes_{\mathbf{Z}} \mathcal{O}_K^2 \cong \mathbf{R}^{2n}$ in which \mathcal{O}_K^2 embeds as a lattice. Then for any positive real number X , the set S_X of elliptic curves $E_{a,b}$ with $\|(a,b)\| < X$ is finite, and we say that *almost all* elliptic curves over K have some property if the fraction of elliptic curves $E_{a,b}$ in S_X having that property tends to 1 when $X \in \mathbf{R}_{>0}$ tends to infinity.

The proof of Theorem 1.1 occupies the next three Sections. We first show, in Section 2, that for any elliptic curve E/K , the connected component $E_{\text{cc}}(\mathbf{A}_K)$ of the zero element is a subgroup of $E(\mathbf{A}_K)$ isomorphic to $(\mathbf{R}/\mathbf{Z})^n$, and that it splits off in the sense that we have a decomposition

$$E(\mathbf{A}_K) \cong E_{\text{cc}}(\mathbf{A}_K) \times E(\mathbf{A}_K)/E_{\text{cc}}(\mathbf{A}_K).$$

The totally disconnected group $E(\mathbf{A}_K)/E_{\text{cc}}(\mathbf{A}_K)$ is profinite and can be analyzed by methods resembling those we employed for the multiplicative group \mathbf{A}_K^* in the class field theoretic setting of [2]. It fits in a split exact sequence

$$0 \rightarrow T_{E/K} \rightarrow E(\mathbf{A}_K)/E_{\text{cc}}(\mathbf{A}_K) \rightarrow \widehat{\mathbf{Z}}^n \rightarrow 0$$

of $\widehat{\mathbf{Z}}$ -modules. Here $T_{E/K}$ is the closure of the torsion subgroup of $E(\mathbf{A}_K)/E_{\text{cc}}(\mathbf{A}_K)$, and we see that we can write $E(\mathbf{A}_K)$ as a product

$$E(\mathbf{A}_K) \cong (\mathbf{R}/\mathbf{Z})^n \times \widehat{\mathbf{Z}}^n \times T_{E/K}$$

in which only $T_{E/K}$ depends on the elliptic curve E/K . The *torsion closure* $T_{E/K}$ is a countable product of finite cyclic groups, and it is shown in Section 3 that $T_{E/K}$ is isomorphic to $\prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$ for those E that satisfy a condition that we formulate after Lemma 3.1 in terms of the division fields associated to E/K . Whether this condition is satisfied can be read off from the Galois representation associated to the torsion points of E , and in Section 4 we use recent results by Jones and Zywna [4, 10] to show that the condition is met for almost all elliptic curves over K , and thus conclude the proof of Theorem 1.1.

The notion of ‘almost all’ from Theorem 1.1 still allows for large numbers of elliptic curves E/K to have adelic point groups *different* from the universal group \mathcal{E}_n . Such non-generic adelic point groups can be characterized by a finite set of prime powers ℓ^k for which cyclic direct summands of order ℓ^k are ‘missing’ from $T_{E/K}$. It is easy (Lemma 5.1) to produce elliptic curves for which $E(\mathbf{A}_K)$ has prescribed missing summands by base changing any given elliptic curve to an appropriate extension field. It is however much harder to construct elliptic curves with non-generic adelic point groups over a *given* number field K . In Theorem 5.4 we show that, for given K , there are only finitely many prime powers ℓ^k for which cyclic direct summands of order ℓ^k can be missing from adelic point groups of elliptic curves E/K . For $K = \mathbf{Q}$, the only prime power turns out to be $\ell^k = 2$, and this can be exploited to prove in our final Theorem 5.6 an explicit version of the following.

Theorem 1.3. *Let K be a number field of degree n . Then there exist infinitely many elliptic curves E/K that are pairwise non-isomorphic over an algebraic closure of K , and for which $E(\mathbf{A}_K)$ is a topological group not isomorphic to \mathcal{E}_n .*

2. STRUCTURE OF ADELIC POINT GROUPS

We let K be a number field of degree n as before, \mathbf{A}_K its adele ring, and E an elliptic curve defined over K . As the K -algebra \mathbf{A}_K is a subring of the full product $\prod_{\mathfrak{p} \leq \infty} K_{\mathfrak{p}}$ of all completions of K , the group $E(\mathbf{A}_K)$ of \mathbf{A}_K -valued points of E naturally embeds into $\prod_{\mathfrak{p} \leq \infty} E(K_{\mathfrak{p}})$. The justification for our earlier definition (2) is the following.

Lemma 2.1. *The natural inclusion $E(\mathbf{A}_K) \longrightarrow \prod_{\mathfrak{p} \leq \infty} E(K_{\mathfrak{p}})$ is an isomorphism.*

Proof. The ring \mathbf{A}_K consists of elements $(x_{\mathfrak{p}})_{\mathfrak{p}}$ that are almost everywhere integral, i.e., for which we have $x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}$ for almost all finite primes \mathfrak{p} of K , with $\mathcal{O}_{\mathfrak{p}} \subset K_{\mathfrak{p}}$ the local ring of integers at \mathfrak{p} . As E can be given by a projective model $E_{a,b}$ as in (1), every $K_{\mathfrak{p}}$ -valued point of E with \mathfrak{p} finite can be written with coordinates in $\mathcal{O}_{\mathfrak{p}}$. It follows that every element in $\prod_{\mathfrak{p} \leq \infty} E(K_{\mathfrak{p}})$ is actually in $E(\mathbf{A}_K)$. \square

As the structure of the point group $E(K_{\mathfrak{p}})$ of an elliptic curve over a local field is different for archimedean and non-archimedean primes, we treat these cases separately.

For archimedean primes \mathfrak{p} of K , the completion $K_{\mathfrak{p}}$ is isomorphic to either \mathbf{R} or \mathbf{C} . At the complex places \mathfrak{p} , the group $E(K_{\mathfrak{p}})$ is a topological group isomorphic to $(\mathbf{R}/\mathbf{Z})^2$, by the well-known fact that we have $E(K_{\mathfrak{p}}) \cong \mathbf{C}/\Lambda$ for some lattice $\Lambda \subset \mathbf{C}$ by the complex analytic theory.

For \mathfrak{p} real, there are two possible types of groups $E(K_{\mathfrak{p}})$, and they may be distinguished by looking at the discriminant Δ_E of the elliptic curve. In the model $E = E(a, b)$ from (1), we have $\Delta_E = \Delta(a, b) = -16(4a^3 + 27b^2) \in K^*$, and changing the Weierstrass model of E will change Δ_E by a 12-th power in K^* , so Δ_E is well-defined as an element of $K^*/(K^*)^{12}$. In particular, the *sign* of $\Delta(E)$ is well-defined for every real prime $\mathfrak{p} : K \rightarrow \mathbf{R}$ of K , and for such \mathfrak{p} we have

$$(3) \quad E(K_{\mathfrak{p}}) \cong \begin{cases} \mathbf{R}/\mathbf{Z}, & \text{if } \Delta_E <_{\mathfrak{p}} 0; \\ \mathbf{R}/\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, & \text{if } \Delta_E >_{\mathfrak{p}} 0. \end{cases}$$

We easily deduce the following.

Proposition 2.2. *Let K be a number field of degree n , and E/K an elliptic curve with discriminant $\Delta_E \in K^*/(K^*)^{12}$. Then we have an isomorphism of topological groups*

$$\prod_{\mathfrak{p}|\infty} E(K_{\mathfrak{p}}) \cong (\mathbf{R}/\mathbf{Z})^n \times (\mathbf{Z}/2\mathbf{Z})^r.$$

Here $r \leq n$ is the number of real primes \mathfrak{p} of K for which we have $\Delta_E >_{\mathfrak{p}} 0$.

Proof. Let K have r_1 real and r_2 complex primes, then $\prod_{\mathfrak{p}|\infty} E(K_{\mathfrak{p}})$ is the product of $r_1 + 2r_2 = n$ circle groups \mathbf{R}/\mathbf{Z} and r copies of $\mathbf{Z}/2\mathbf{Z}$, with $r \leq r_1 \leq n$. \square

For a result for the non-archimedean part $\prod_{\mathfrak{p}<\infty} E(K_{\mathfrak{p}})$ of $E(\mathbf{A}_K)$ analogous to Proposition 2.2, we first describe $E(K_{\mathfrak{p}})$ for a single finite prime \mathfrak{p} of K . Suppose that E is given by a Weierstrass model as in (1), and consider the continuous reduction map

$$(4) \quad \phi_{\mathfrak{p}} : E(K_{\mathfrak{p}}) \longrightarrow \overline{E}(k_{\mathfrak{p}})$$

from $E(K_{\mathfrak{p}})$ to the finite set of points of the curve \overline{E} described by the reduced Weierstrass equation over the residue class field $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$. By Hensel's lemma, the set of points in the non-singular locus $\overline{E}^{\text{ns}}(k_{\mathfrak{p}})$ of \overline{E} is contained in the image of ϕ , and it inherits a natural group structure from $E(K_{\mathfrak{p}})$. Writing $E_0(K_{\mathfrak{p}}) = \phi^{-1}[\overline{E}^{\text{ns}}(k_{\mathfrak{p}})]$, we obtain an exact sequence of topological groups

$$(5) \quad 1 \rightarrow E_1(K_{\mathfrak{p}}) \longrightarrow E_0(K_{\mathfrak{p}}) \longrightarrow \overline{E}^{\text{ns}}(k_{\mathfrak{p}}) \rightarrow 1.$$

The kernel of reduction $E_1(K_{\mathfrak{p}})$ is a subgroup of finite index in $E_0(K_{\mathfrak{p}})$.

For primes of good reduction, we have $E_0(K_{\mathfrak{p}}) = E(K_{\mathfrak{p}})$, and $\overline{E}^{\text{ns}}(k_{\mathfrak{p}}) = \overline{E}(k_{\mathfrak{p}})$ is the point group of the elliptic curve $\overline{E} = (E \bmod \mathfrak{p})$ over $k_{\mathfrak{p}}$. In this case, the exact sequence (5) becomes

$$(6) \quad 1 \rightarrow E_1(K_{\mathfrak{p}}) \longrightarrow E(K_{\mathfrak{p}}) \longrightarrow \overline{E}(k_{\mathfrak{p}}) \rightarrow 1.$$

For primes of bad reduction, $E_0(K_{\mathfrak{p}})$ is a strict subgroup of $E(K_{\mathfrak{p}})$, but it is of finite index in $E(K_{\mathfrak{p}})$ by [9, Chapter VII, Corollary 6.2]. In all cases, $E_1(K_{\mathfrak{p}})$ is a subgroup of finite index in $E(K_{\mathfrak{p}})$.

Lemma 2.3. *Let \mathfrak{p} be a prime of K lying over p . Then the torsion subgroup $T_{\mathfrak{p}} \subset E(K_{\mathfrak{p}})$ is finite abelian, and $E(K_{\mathfrak{p}})/T_{\mathfrak{p}}$ is a free \mathbf{Z}_p -module of rank $[K_{\mathfrak{p}} : \mathbf{Q}_p]$.*

Proof. The kernel of reduction $E_1(K_{\mathfrak{p}})$ is a pro- p -group that we can describe as a \mathbf{Z}_p -module using the formal group of E as in [9, Chapter IV]. More precisely, the elliptic logarithm

$$\log_{\mathfrak{p}} : E_1(K_{\mathfrak{p}}) \rightarrow \mathcal{O}_{\mathfrak{p}}$$

has finite kernel of p -power order and maps $E_1(K_{\mathfrak{p}})$ onto an open additive subgroup of the valuation ring $\mathcal{O}_{\mathfrak{p}} \subset K_{\mathfrak{p}}$. This shows that, just like $\mathcal{O}_{\mathfrak{p}}$ itself, $E_1(K_{\mathfrak{p}})$ is a finitely generated \mathbf{Z}_p -module of free rank $[K_{\mathfrak{p}} : \mathbf{Q}_p]$. As $E_1(K_{\mathfrak{p}})$ is of finite index in $E(K_{\mathfrak{p}})$, we find that the p -primary part of $E(K_{\mathfrak{p}})$ is also a finitely generated \mathbf{Z}_p -module of free rank $[K_{\mathfrak{p}} : \mathbf{Q}_p]$. The non- p part of $E(K_{\mathfrak{p}})$ is a finite group of order coprime to p . We can non-canonically write

$$(7) \quad E(K_{\mathfrak{p}}) \cong \mathbf{Z}_p^{[K_{\mathfrak{p}} : \mathbf{Q}_p]} \times T_{\mathfrak{p}},$$

with $T_{\mathfrak{p}}$ the finite torsion group of $E(K_{\mathfrak{p}})$. \square

Taking the product in (7) over all non-archimedean primes \mathfrak{p} of K , and using the fact that the sum of the local degrees at the primes over p in K equals $n = [K : \mathbf{Q}]$, we obtain the following non-archimedean analogue of Proposition 2.2.

Proposition 2.4. *Let E be an elliptic curve over a number field K of degree n . Then we have an isomorphism of topological groups*

$$\prod_{\mathfrak{p} < \infty} E(K_{\mathfrak{p}}) = \widehat{\mathbf{Z}}^n \times \prod_{\mathfrak{p} < \infty} T_{\mathfrak{p}},$$

where $T_{\mathfrak{p}} = E(K_{\mathfrak{p}})^{\text{tor}}$ is the finite torsion subgroup of $E(K_{\mathfrak{p}})$. \square

We may combine the Propositions 2.2 and 2.4 for the infinite and the finite primes into a single statement for the adelic point group $E(\mathbf{A}_K)$ by putting

$$(8) \quad T_{\mathfrak{p}} = \begin{cases} E(K_{\mathfrak{p}})^{\text{tor}} & \text{if } \mathfrak{p} \text{ is finite;} \\ \mathbf{Z}/2\mathbf{Z} & \text{if } \mathfrak{p} \text{ is real and } \Delta_E >_{\mathfrak{p}} 0; \\ 1 & \text{otherwise.} \end{cases}$$

With this definition of $T_{\mathfrak{p}}$, we obtain an isomorphism of topological groups

$$(9) \quad E(\mathbf{A}_K) \cong (\mathbf{R}/\mathbf{Z})^n \times \widehat{\mathbf{Z}}^n \times \prod_{\mathfrak{p} \leq \infty} T_{\mathfrak{p}}.$$

Note that in this decomposition, $(\mathbf{R}/\mathbf{Z})^n$ represents the connected component $E_{\text{cc}}(\mathbf{A}_K)$ of the zero element in $E(\mathbf{A}_K)$. In the totally disconnected profinite group

$$E(\mathbf{A}_K)/E_{\text{cc}}(\mathbf{A}_K) \cong \widehat{\mathbf{Z}}^n \times \prod_{\mathfrak{p} \leq \infty} T_{\mathfrak{p}},$$

the profinite subgroup

$$(10) \quad T_{E/K} = \prod_{\mathfrak{p} \leq \infty} T_{\mathfrak{p}}$$

can be intrinsically defined as the topological *closure* of the torsion subgroup of $E(\mathbf{A}_K)/E_{\text{cc}}(\mathbf{A}_K)$. The quotient $(E(\mathbf{A}_K)/E_{\text{cc}}(\mathbf{A}_K))/T_{E/K}$ is a free $\widehat{\mathbf{Z}}$ -module of rank n .

By the isomorphism (9), the structure of $E(\mathbf{A}_K)$ as a topological group is determined by the degree n of the number field K and the isomorphism type of the *torsion closure* $T_{E/K} \subset E(\mathbf{A}_K)/E_{\text{cc}}(\mathbf{A}_K)$, which we will describe now.

3. STRUCTURE OF THE TORSION CLOSURE

Let T be any group that is obtained as a countable product of finite abelian or, equivalently, finite cyclic groups. Then there are usually many ways to represent the group T as such a product. The group $\prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$ occurring in Theorem 1.1 is for instance isomorphic to $\prod_{m=2017}^{\infty} \mathbf{Z}/m\mathbf{Z}$, to $(\prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z})^2$, and even to $\prod_p \mathbf{F}_p^*$. Our representation in the Theorem is simply a choice that requires only a few characters to write it down.

In order to describe a countable product T of finite cyclic groups in a more canonical way, one can write each of the cyclic constituents of T as a product of cyclic groups of prime power order, and arrive at the *standard representation*

$$(11) \quad T = \prod_{\ell \text{ prime}} \prod_{k=1}^{\infty} (\mathbf{Z}/\ell^k \mathbf{Z})^{e(\ell^k)}$$

for T . The exponent $e(\ell^k)$ in this representation can intrinsically be defined in terms of T as

$$(12) \quad e(\ell^k) = \dim_{\mathbf{F}_\ell} T[\ell^k] / (T[\ell^{k-1}] + \ell T[\ell^{k+1}]),$$

and is known as the ℓ^k -rank of T . Two countable products of finite cyclic groups are isomorphic if and only if their ℓ^k -ranks coincide for *all* prime powers $\ell^k > 1$.

The \mathbf{F}_ℓ -dimensions $e(\ell^k)$ in (12) are either finite, in which case $e(\ell^k)$ is a non-negative integer, or countably infinite. In the latter case we write $e(\ell^k) = \omega$, and note that the group

$$(\mathbf{Z}/\ell^k \mathbf{Z})^\omega = \text{Map}(\mathbf{Z}_{>0}, \mathbf{Z}/\ell^k \mathbf{Z})$$

can be identified with the group of $\mathbf{Z}/\ell^k \mathbf{Z}$ -valued functions on the countable set $\mathbf{Z}_{>0}$ of positive integers.

In the case where we have $e(\ell^k) = \omega$ for *all* prime powers ℓ^k , we are dealing with the group $\prod_{m=1}^{\infty} \mathbf{Z}/m \mathbf{Z}$ occurring in Theorem 1.1. Thus, the key to proving Theorem 1.1 lies in showing that for almost all E , the torsion closure $T_{E/K}$ in (10) associated to E/K has infinite ℓ^k -rank for *all* prime powers $\ell^k > 1$.

In order to determine the ℓ^k -rank of $T_{E/K}$, we need to determine how many cyclic direct summands of order ℓ^k occur in the finite local torsion groups $T_{\mathfrak{p}} = E(K_{\mathfrak{p}})^{\text{tor}}$ at the non-archimedean primes \mathfrak{p} of K . This can be done by studying the splitting behavior of the finite primes of K in the ℓ^k -division fields

$$(13) \quad Z_{E/K}(\ell^k) \stackrel{\text{def}}{=} K(E[\ell^k](\overline{K}))$$

of the elliptic curve E over K . The field $Z_{E/K}(\ell^k)$ is the finite Galois extension of K obtained by adjoining to K the coordinates of all ℓ^k -torsion points of E in an algebraic closure \overline{K} of K . The ℓ^k -torsion subgroup $E(K_{\mathfrak{p}})[\ell^k] \subset T_{\mathfrak{p}} \subset E(K_{\mathfrak{p}})$ of E over $K_{\mathfrak{p}}$ is *full*, i.e., isomorphic to the group $E(\overline{K})[\ell^k] \cong (\mathbf{Z}/\ell^k \mathbf{Z})^2$, if and only if \mathfrak{p} splits completely in the extension $K \subset Z_{E/K}(\ell^k)$. This leads to the following criterion for $T_{E/K}$ to have (countably) infinite ℓ^k -rank.

Lemma 3.1. *Let E/K be an elliptic curve, and $\ell^k > 1$ a prime power for which the inclusion*

$$Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$$

of division fields is strict. Then the torsion closure $T_{E/K}$ has infinite ℓ^k -rank.

Proof. Let \mathfrak{p} be a finite prime of K that splits completely in the division field $Z_{E/K}(\ell^k)$, but not in the division field $Z_{E/K}(\ell^{k+1})$. Then $E(K_{\mathfrak{p}})$ has full ℓ^k -torsion, but not full ℓ^{k+1} -torsion. This implies that the finite group $T_{\mathfrak{p}}$ contains a subgroup isomorphic to $(\mathbf{Z}/\ell^k \mathbf{Z})^2$ but not one isomorphic to $(\mathbf{Z}/\ell^{k+1} \mathbf{Z})^2$, and therefore has at least one cyclic direct summand of order ℓ^k .

By our assumption, the set of primes \mathfrak{p} that split completely in $Z_{E/K}(\ell^k)$, but not in $Z_{E/K}(\ell^{k+1})$, is infinite and of positive density

$$[Z_{E/K}(\ell^k) : K]^{-1} - [Z_{E/K}(\ell^{k+1}) : K]^{-1} > 0.$$

For all \mathfrak{p} in the infinite set thus obtained, the group $T_{\mathfrak{p}}$ has a cyclic direct summand of order ℓ^k . It follows that $T_{E/K} = \prod_{\mathfrak{p} \leq \infty} T_{\mathfrak{p}}$ has infinite ℓ^k -rank. \square

We conclude from Lemma 3.1 that for an elliptic curve E having the property that for all primes ℓ , the tower of ℓ -power division fields

$$(14) \quad Z_{E/K}(\ell) \subset Z_{E/K}(\ell^2) \subset Z_{E/K}(\ell^3) \subset \cdots \subset Z_{E/K}(\ell^k) \subset \cdots$$

has strict inclusions at every level, the group $T_{E/K}$ is isomorphic to the group $\prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$ having infinite ℓ^k -rank for all prime powers ℓ^k . In this situation, the adelic point group $E(\mathbf{A}_K)$ of E is isomorphic to the universal group

$$(15) \quad \mathcal{E}_n = (\mathbf{R}/\mathbf{Z})^n \times \widehat{\mathbf{Z}}^n \times \prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z},$$

in degree n , and we are dealing with an elliptic curve E over K that is ‘generic’ in the sense of Theorem 1.1.

4. UNIVERSALITY OF \mathcal{E}_n

In order to finish the proof of Theorem 1.1, it now suffices to show that for ‘almost all’ (in the sense of the theorem) elliptic curves E defined over a fixed number field K , the extension $Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$ in the tower (14) of ℓ -power division fields is strict for *all* prime powers $\ell^k > 1$. In order to see whether this condition is satisfied for a given elliptic curve E over K , we look at its associated Galois representation

$$(16) \quad \rho_E : G_K = \text{Gal}(\overline{K}/K) \longrightarrow \mathfrak{A}_K = \text{Aut}(E(\overline{K})^{\text{tor}})$$

describing the action of the absolute Galois group of K on the group $E(\overline{K})^{\text{tor}}$ of \overline{K} -valued torsion points of E . As $E(\overline{K})^{\text{tor}}$ is an injective limit

$$E(\overline{K})^{\text{tor}} = \varinjlim E(\overline{K})[m] \cong \varinjlim \left(\frac{1}{m} \mathbf{Z}/\mathbf{Z} \right)^2 = (\mathbf{Q}/\mathbf{Z})^2,$$

its automorphism group \mathfrak{A}_K can be (non-canonically) identified with the profinite group $\varprojlim_n \text{GL}_2(\mathbf{Z}/m\mathbf{Z}) = \text{GL}_2(\widehat{\mathbf{Z}})$. The composition

$$\phi = \det \circ \rho_E : G_K \rightarrow \widehat{\mathbf{Z}}^*$$

does not depend on a choice of basis and gives the action of G_K on the maximal cyclotomic extension $K \subset K^{\text{cyc}} = K(\zeta_{\infty})$ of K : for $\sigma \in G_K$ and ζ a root of unity, we have $\sigma(\zeta) = \zeta^{\phi(\sigma)}$.

The restriction of the action of G_K to the m -torsion subgroup $E(\overline{K})[m]$ of $E(\overline{K})^{\text{tor}}$ is described by the reduction

$$\rho_{E,m} : G_K \longrightarrow \text{Aut}(E(\overline{K})[m]) \cong \text{GL}_2(\mathbf{Z}/m\mathbf{Z})$$

of ρ_E modulo m , and the invariant field of $\ker \rho_{E,m}$ is precisely the m -division field $Z_{E/K}(m) = K(E(\overline{K})[m])$ of E over K . In particular, we have an equivalence

$$(17) \quad Z_{E/K}(\ell^k) = Z_{E/K}(\ell^{k+1}) \iff \ker[\rho_{E,\ell^k}] = \ker[\rho_{E,\ell^{k+1}}].$$

In case the map ρ_E in (16) is *surjective*, all extensions $Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$ have degree

$$(18) \quad \ell^4 = \# \ker[\text{GL}_2(\mathbf{Z}/\ell^{k+1}\mathbf{Z}) \longrightarrow \text{GL}_2(\mathbf{Z}/\ell^k\mathbf{Z})],$$

and in this case $E(\mathbf{A}_K)$ is isomorphic to the universal group \mathcal{E}_n in (15).

It is certainly not true that the *image of Galois* $\rho_E[G_K]$ is always equal to the full automorphism group $\mathfrak{A}_K = \text{Aut}(E(\overline{K})^{\text{tor}})$. There is however the basic result, due to Serre [8], that $\rho_E[G_K]$ is an *open* subgroup of \mathfrak{A}_K if E is *without CM*, i.e., if E does *not* have complex multiplication over \overline{K} . In particular, the index of $\rho_E[G_K]$ in $\mathfrak{A}_K \cong \text{GL}_2(\widehat{\mathbf{Z}})$ is always finite for E without CM. As elliptic curves defined over

K with CM over \bar{K} have their j -invariants in some *finite* subset of K , almost all elliptic curves over K are without CM.

We first look at the case $K = \mathbf{Q}$, which is somewhat particular as there is a special complication for \mathbf{Q} that prevents ρ_E in all cases from being surjective. In order to describe it, we let

$$\chi_2 : \mathfrak{A}_{\mathbf{Q}} = \text{Aut}(E(\bar{\mathbf{Q}})^{\text{tor}}) \longrightarrow \text{Aut}(E[2](\bar{\mathbf{Q}})) \cong \text{GL}_2(\mathbf{Z}/2\mathbf{Z}) \cong S_3 \rightarrow \{\pm 1\}$$

be the non-trivial quadratic character that maps an automorphism of $E(\bar{\mathbf{Q}})^{\text{tor}}$ to the sign of the permutation by which it acts on the three non-trivial 2-torsion points of E . For $\sigma \in G_{\mathbf{Q}}$, the sign of this permutation for $\rho_E(\sigma)$ is reflected in the action of σ on the subfield $\mathbf{Q}(\sqrt{\Delta}) \subset Z_{E/K}(2)$ that is generated by the square root of the discriminant $\Delta = \Delta_E$ of the elliptic curve E , and given by

$$\chi_2(\rho_E(\sigma)) = \sigma(\sqrt{\Delta})/\sqrt{\Delta}.$$

The Dirichlet character $\hat{\mathbf{Z}}^* \rightarrow \{\pm 1\}$ corresponding to $\mathbf{Q}(\sqrt{\Delta})$ can be seen as a character

$$\chi_{\Delta} : \mathfrak{A}_{\mathbf{Q}} \cong \text{GL}_2(\hat{\mathbf{Z}}) \xrightarrow{\det} \hat{\mathbf{Z}}^* \rightarrow \{\pm 1\}$$

on $\mathfrak{A}_{\mathbf{Q}}$. It is different from the character χ_2 , which does not factor via the determinant map $\mathfrak{A}_{\mathbf{Q}} \xrightarrow{\det} \hat{\mathbf{Z}}^*$ on $\mathfrak{A}_{\mathbf{Q}}$.

The *Serre character* $\chi_E : \mathfrak{A}_{\mathbf{Q}} \rightarrow \{\pm 1\}$ associated to E is the non-trivial quadratic character obtained as the product $\chi_E = \chi_2 \chi_{\Delta}$. By construction, it vanishes on the image of Galois $\rho_E(G_{\mathbf{Q}}) \subset \mathfrak{A}_{\mathbf{Q}}$, so the image of Galois is never the full group $\mathfrak{A}_{\mathbf{Q}}$. In the case where we have $\rho_E(G_{\mathbf{Q}}) = \ker[\chi_E]$, we say that E is a *Serre curve*.

If E is a Serre curve, then the image of Galois is of index 2 in the full group $\mathfrak{A}_{\mathbf{Q}} \cong \text{GL}_2(\hat{\mathbf{Z}})$, and for every prime power $\ell^k > 1$, the extension

$$Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$$

of division fields for E that occurs in Lemma 3.1 has the ‘generic’ degree ℓ^4 from (18) for odd ℓ , and at least degree ℓ^3 for $\ell = 2$. In particular, the hypothesis of Lemma 3.1 on E is satisfied for all prime powers ℓ^k in case E is a Serre curve. Nathan Jones [4] proved in 2010 that, in the sense of our Theorem 1.1, almost all elliptic curves are Serre curves. This immediately implies the following special case of Theorem 1.1, which can already be found in [1].

Theorem 4.1. *For almost all elliptic curves E/\mathbf{Q} , the adelic point group $E(\mathbf{A}_{\mathbf{Q}})$ is isomorphic to the topological group*

$$\mathcal{E}_1 = \mathbf{R}/\mathbf{Z} \times \hat{\mathbf{Z}} \times \prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}. \quad \square$$

In order to deal with number fields K different from \mathbf{Q} , we need an analogue of Jones’ result stating that for almost all E over K , the image of Galois $\rho_E[G_K] \subset \mathfrak{A}_K$ is as large as it can possibly be. As quadratic extensions of a number field $K \neq \mathbf{Q}$ will ‘generically’ not be cyclotomic, there is no Serre character for such K . However, for number fields K that are not linearly disjoint from the maximal cyclotomic extension $\mathbf{Q}^{\text{cyc}} = \mathbf{Q}(\zeta_{\infty})$ of \mathbf{Q} , the natural embedding

$$\text{Gal}(K^{\text{cyc}}/K) \longrightarrow \text{Gal}(\mathbf{Q}^{\text{cyc}}/\mathbf{Q}) = \hat{\mathbf{Z}}^*$$

will not be an isomorphism, and identify $\text{Gal}(K^{\text{cyc}}/K)$ with some open subgroup $H_K \subset \widehat{\mathbf{Z}}^*$ of index equal to the field degree of the extension $\mathbf{Q} \subset (K \cap \mathbf{Q}^{\text{cyc}})$. In this case, the image of Galois $\rho_E[G_K] \subset \mathfrak{A}_K$ is contained in the inverse image $\det^{-1}[H_K]$ of H_K under the determinant map $\det : \mathfrak{A}_K \rightarrow \widehat{\mathbf{Z}}^*$. We say that the image of Galois for an elliptic curve E over $K \neq \mathbf{Q}$ is *maximal* in case we have

$$(19) \quad \rho_E[G_K] = \det^{-1}[H_K].$$

We want almost all (in the sense of our Theorem 4.1) elliptic curves to have maximal Galois image, and this is exactly what Zywinia proved in 2010.

Theorem 4.2. (Zywinia [10]) *Almost all elliptic curves over a number field $K \neq \mathbf{Q}$ have maximal Galois image.* \square

We can now finish the proof of our main theorem.

Proof of Theorem 1.1. In the case $K = \mathbf{Q}$, almost all elliptic curves E/K are Serre curves, and we are in the special case of Theorem 4.1.

For $K \neq \mathbf{Q}$, almost all elliptic curves E over K have maximal Galois image by Theorem 4.2, and this implies in particular that

$$\rho_E[G_K] = \det^{-1}[H_K] \subset \mathfrak{A}_K$$

contains $\ker[\det] \cong \text{SL}_2(\widehat{\mathbf{Z}})$ for these E . It follows that for prime powers $\ell^k > 1$, the degree of the extension $Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$ for these E is maybe not the maximal possible degree ℓ^4 that we have in (18), but it is still at least

$$(20) \quad \ell^3 = \# \ker[\text{SL}_2(\mathbf{Z}/\ell^{k+1}\mathbf{Z}) \rightarrow \text{SL}_2(\mathbf{Z}/\ell^k\mathbf{Z})].$$

This implies that the group $T_{E/K}$ from (10) is the ‘maximal’ group $\prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$, and from (8) we then see that the adelic point group $E(\mathbf{A}_K)$ is isomorphic to the universal group \mathcal{E}_n , as was to be shown. \square

5. NON-GENERIC POINT GROUPS

The proof of Theorem 1.1 uses the fact for almost all elliptic curves E over a fixed number field K of degree n , the inclusion of division fields

$$(21) \quad Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$$

is strict for all prime powers ℓ^k , making $E(\mathbf{A}_K)$ by Lemma 3.1 into the generic adelic point group \mathcal{E}_n . The adelic point group of an elliptic curve E/K is non-generic if and only if the torsion closure $T_{E/K}$ in the representation

$$E(\mathbf{A}_K) \cong (\mathbf{R}/\mathbf{Z})^n \times \widehat{\mathbf{Z}}^n \times T_{E/K}$$

(cf. (9) and (10)) does *not* have infinite ℓ^k -rank for one or more prime powers ℓ^k . For these exceptional prime powers, the inclusion (21) has to be an equality.

In case we can freely choose our ground field K , it is easy to force equality in (21), and to produce elliptic curves E/K for which the torsion closure $T_{E/K}$ has ℓ^k -rank equal to 0 for *any* prescribed finite set of prime powers ℓ^k . It suffices to take m sufficiently large in the following Lemma.

Lemma 5.1. *Let E/\mathbf{Q} be any elliptic curve, $m \in \mathbf{Z}_{>0}$ an integer, and*

$$K = Z_{E/\mathbf{Q}}(m) = \mathbf{Q}(E[m](\overline{\mathbf{Q}}))$$

the m -division field of E over \mathbf{Q} . Then E is an elliptic curve defined over K , and $T_{E/K}$ has ℓ^k -rank 0 for every prime power $\ell^k > 1$ for which ℓ^{k+1} divides m .

Proof. Suppose $\ell^{k+1} > \ell$ divides m . Then the full ℓ^{k+1} -torsion subgroup $E(\overline{K})[\ell^{k+1}]$ is contained in $E(K)$, so none of the torsion subgroups $T_{\mathfrak{p}}$ of the non-archimedean point groups $E(K_{\mathfrak{p}})$ in (7) will have a cyclic direct summand of order ℓ^k . As K contains an ℓ^{k+1} -th root of unity it has no real primes, and by definition (8) the torsion closure $T_{E/K} = \prod_{\mathfrak{p} \leq \infty} T_{\mathfrak{p}}$ has ℓ^k -rank 0. \square

In view of Lemma 5.1, a more interesting question is which non-generic adelic point groups can occur over a *given* number field K , such as $K = \mathbf{Q}$. To realize non-generic adelic point groups, we need elliptic curves E/K and primes ℓ for which the tower of ℓ -power division fields

$$(22) \quad Z_{E/K}(\ell) \subset Z_{E/K}(\ell^2) \subset Z_{E/K}(\ell^3) \subset \cdots \subset Z_{E/K}(\ell^k) \subset \cdots$$

from (14) does not have strict inclusions at every level.

To ease notation, we write $G_{\ell^k} = \text{Gal}(Z_{E/K}(\ell^k)/K)$ for the Galois group over K of the ℓ^k -division field, and $M_{\ell^k} = E[\ell^k](\overline{K})$ for the group of ℓ^k -torsion points of $E(\overline{K})$. As M_{ℓ^k} is free of rank 2 over $\mathbf{Z}/\ell^k\mathbf{Z}$ and G_{ℓ^k} acts faithfully on M_{ℓ^k} , we have an inclusion

$$(23) \quad G_{\ell^k} \subset \text{Aut}(M_{\ell^k}) \cong \text{GL}_2(\mathbf{Z}/\ell^k\mathbf{Z}),$$

and we can view $\lim_{\leftarrow k} G_{\ell^k}$ as a subgroup of $\text{Aut}(\lim_{\rightarrow k} M_{\ell^k}) \cong \text{GL}_2(\mathbf{Z}_{\ell})$.

The Galois group of the $(k-1)$ -st extension in the tower (22) is the ℓ -group arising as the kernel

$$(24) \quad K_{\ell^k} = \ker[G_{\ell^k} \rightarrow G_{\ell^{k-1}}] \quad (k \geq 2)$$

of the surjection induced by the restriction map $\varphi_{\ell^k} : \text{Aut}(M_{\ell^k}) \rightarrow \text{Aut}(M_{\ell^{k-1}})$, so we have

$$(25) \quad K_{\ell^{k+1}} = 1 \iff Z_{E/K}(\ell^k) = Z_{E/K}(\ell^{k+1}).$$

As we will show now, the triviality of the kernels $K_{\ell^{k+1}}$ needed to obtain non-generic point groups can only arise for a finite number of initial values of $k \geq 1$, with $\ell = 2$ playing a special role.

Proposition 5.2. *Let ℓ be an odd prime, and suppose $K_{\ell^N} \neq 1$ for some $N \geq 2$. Then we have $K_{\ell^k} \neq 1$ for all $k > N$. For $\ell = 2$, the same is true if we have $N \geq 3$.*

Proof. Write $\sigma_N \in K_{\ell^N} \setminus \{1\}$ for $N \geq 2$ as $\sigma_N = 1 + \ell^{N-1}x$ with $x \neq \ell y \in \text{End}(M_{\ell^N})$. If $\sigma_k \in G_{\ell^k}$ for $k > N$ maps to σ_N under the restriction map $G_{\ell^k} \twoheadrightarrow G_{\ell^N}$, we have $\sigma_k = 1 + \ell^{N-1}x_k$ with $x_k \neq \ell y_k \in \text{End}(M_{\ell^k})$, and

$$(26) \quad \sigma_k^{\ell} = 1 + \ell^N x_k + \sum_{i=2}^{\ell} \binom{\ell}{i} \ell^{i(N-1)} x_k^i = 1 + \ell^N x_k \in \text{End}(M_{\ell^k}).$$

Indeed, the number of factors ℓ in the coefficient $\binom{\ell}{i} \ell^{i(N-1)}$ is for $i = 2, 3, \dots, \ell-1$ at least $1 + 2(N-1) \geq N+1$ if we have $N \geq 2$, and for $i = \ell$ in the final coefficient $\ell^{\ell(N-1)}$ it is $\ell(N-1) \geq N+1$ if we either have $\ell \geq 3, N \geq 2$ or $\ell = 2, N \geq 3$. Assuming we are in this situation, we see that σ_k^{ℓ} is in $K_{\ell^{N+1}} \setminus \{1\}$. Repeating the argument, we find that if σ_k is raised $k-N$ times to the power ℓ , we end up with an element $1 + \ell^{k-1}x_k \in K_{\ell^k} \setminus \{1\}$, showing $K_{\ell^k} \neq 1$. \square

In view of Proposition 5.2, it makes sense to focus on the kernels K_{ℓ^2} and K_8 in (24).

Proposition 5.3. *Suppose K is a number field linearly disjoint from the ℓ^2 -th cyclotomic field $\mathbf{Q}(\zeta_{\ell^2})$, with ℓ an odd prime. Then for all elliptic curves E/K , the tower (22) has strict inclusions at all levels.*

Proof. By Proposition 5.2, it suffices to show that $K_{\ell^2} = \ker[\pi : G_{\ell^2} \rightarrow G_{\ell}]$ is non-trivial for all elliptic curves E/K . By the hypothesis on K , the determinant map $G_{\ell^2} \xrightarrow{\det} (\mathbf{Z}/\ell^2\mathbf{Z})^*$ is surjective. As ℓ is odd, we can pick $c \in G_{\ell^2}$ such that $\det(c)$ generates $(\mathbf{Z}/\ell^2\mathbf{Z})^*$. Applying π , we find that $\det(\pi(c))$ generates $\mathbf{F}_{\ell}^* = (\mathbf{Z}/\ell\mathbf{Z})^*$.

Suppose that K_{ℓ^2} is trivial, making π an isomorphism. Then the order of $\pi(c)$ equals the order of c , which is divisible by the order $\ell(\ell - 1)$ of $(\mathbf{Z}/\ell^2\mathbf{Z})^*$. Let $s \in G_{\ell}$ be a power of $\pi(c)$ of order ℓ . Then $s \in G_{\ell} \subset \text{Aut}(M_{\ell}) \cong \text{GL}_2(\mathbf{F}_{\ell})$, when viewed as a 2×2 -matrix over the field \mathbf{F}_{ℓ} , is a non-semisimple matrix with double eigenvalue 1. As $\pi(c)$ centralizes this element, its eigenvalues cannot be distinct, and we find that $\det(\pi(c))$ is a square in \mathbf{F}_{ℓ}^* . Contradiction. (This neat argument is due to Hendrik Lenstra.) \square

We can now show that, in contrast to Lemma 5.1, there are only few ways in which adelic point groups of E/K can be non-generic if we fix the base field K .

Theorem 5.4. *Let K be a number field. Then there exists a finite set Σ_K of powers of primes $\ell \mid 2 \cdot \text{disc}(K)$ such that for every elliptic curve E/K and for every prime power $\ell^k \notin \Sigma_K$, the closure of torsion $T_{E/K} \subset E(\mathbf{A}_K)$ has infinite ℓ^k -rank.*

Proof. Suppose there exists a prime power ℓ^k and an elliptic curve E/K for which T_E does not have infinite ℓ^k -rank. Then we have $K_{\ell^{k+1}} = 1$ in (25) for the associated tower (22). If ℓ is odd, K is not linearly disjoint from $\mathbf{Q}(\zeta_{\ell^2})$ by Proposition 5.3, so ℓ divides $\text{disc}(K)$. This leaves us with finitely many possibilities for ℓ .

If ℓ is odd, we have $K_{\ell^N} = 1$ for $2 \leq N \leq k+1$ by Proposition 5.2, hence

$$(27) \quad Z_{E/K}(\ell^{k+1}) = Z_{E/K}(\ell).$$

As $Z_{E/K}(\ell^{k+1})$ contains a primitive ℓ^{k+1} -st root of unity and $Z_{E/K}(\ell)$ is of degree at most $\#\text{GL}_2(\mathbf{F}_{\ell}) < \ell^4$ over K , we can effectively bound k , say by $3 + \text{ord}_{\ell}(n)$, for K of degree n . For $\ell^k = 2^k > 4$, the argument is similar, using $Z_{E/K}(2^{k+1}) = Z_{E/K}(4)$ instead of (27). \square

The proof of Theorem 5.4 is constructive and yields a set Σ_K of prime powers ℓ^k , but it does not automatically yield the *minimal* set.

For $K = \mathbf{Q}$, one can take $\Sigma_{\mathbf{Q}}$ containing only powers of $\ell = 2$, and simple Galois theory shows that $\Sigma_{\mathbf{Q}} = \{2, 4, 8\}$ is actually large enough: no equality

$$Z_{E/K}(2^{k+1}) = Z_{E/K}(4)$$

can hold for $k \geq 4$, as $Z_{E/K}(2^{k+1})$ then contains a cyclic subfield $\mathbf{Q}(\zeta_{32} + \zeta_{32}^{-1})$ of degree 8 over \mathbf{Q} , whereas $G_4 = \text{Gal}(Z_{E/K}(4)/\mathbf{Q}) \subset \text{GL}_2(\mathbf{Z}/4\mathbf{Z})$ has no elements of order divisible by 8. It is relatively easy to show that the minimal set $\Sigma_{\mathbf{Q}}$ does contain 2, as there is the following classical construction of a family of elliptic curves E/\mathbf{Q} for which we have $Z_{E/\mathbf{Q}}(2) = Z_{E/\mathbf{Q}}(4)$.

Proposition 5.5. *For every $r \in \mathbf{Q}^*$, the elliptic curve*

$$E_r : y^2 = x(x^2 - 2(1 - 4r^4)x + (1 + 4r^4)^2)$$

has division fields $Z_{E_r/\mathbf{Q}}(2) = Z_{E_r/\mathbf{Q}}(4) = \mathbf{Q}(i)$. Conversely, every elliptic curve E/\mathbf{Q} with $Z_{E/\mathbf{Q}}(2) = Z_{E/\mathbf{Q}}(4) = \mathbf{Q}(i)$ is \mathbf{Q} -isomorphic to E_r for some $r \in \mathbf{Q}^$.*

Proof. Let E/\mathbf{Q} be defined by a Weierstrass equation $y^2 = f(x)$, and suppose that we have $Z_{E/\mathbf{Q}}(2) = Z_{E/\mathbf{Q}}(4) = \mathbf{Q}(i)$. Then $f \in \mathbf{Q}[x]$ is a monic cubic polynomial with splitting field $Z_{E/\mathbf{Q}}(2) = \mathbf{Q}(i)$, so f has one rational root, and two complex conjugate roots in $\mathbf{Q}(i) \setminus \mathbf{Q}$. After translating x over the rational root, we may take 0 to be the rational root of f , leading to the model

$$(28) \quad E : f(x) = x(x - \alpha)(x - \bar{\alpha})$$

for some element $\alpha \in \mathbf{Q}(i) \setminus \mathbf{Q}$. Note that each such α does define an elliptic curve over \mathbf{Q} , and that the \mathbf{Q} -isomorphism class of E depends on α up to conjugation and up to multiplication by the square of a non-zero rational number.

The equality $Z_{E/\mathbf{Q}}(4) = \mathbf{Q}(i)$ means that the 4-torsion of E is defined over $\mathbf{Q}(i)$, or, equivalently, that the 2-torsion subgroup $E[2](\mathbf{Q}(i))$ of E is contained in $2 \cdot E(\mathbf{Q}(i))$. In terms of the complete 2-descent map [9, Proposition 1.4, p. 315] over $K = \mathbf{Q}(i)$, which embeds $E(K)/2E(K)$ in a subgroup of $K^*/(K^*)^2 \times K^*/(K^*)^2$, the inclusion $E[2](\mathbf{Q}(i)) \subset 2 \cdot E(\mathbf{Q}(i))$ amounts to the statement that all differences between the roots of f are squares in $\mathbf{Q}(i)$. In other words, we have $Z_{E/\mathbf{Q}}(2) = Z_{E/\mathbf{Q}}(4) = \mathbf{Q}(i)$ if and only if α and $\alpha - \bar{\alpha}$ are squares in $\mathbf{Q}(i)$.

Writing $\alpha = (a + bi)^2$ with $ab \neq 0$, we can scale $a + bi$ inside the \mathbf{Q} -isomorphism class of E by an element of \mathbf{Q}^* , and flip signs of a and b . Thus we may take $\alpha = (1 + qi)^2$, with q a positive rational number. The fact that $\alpha - \bar{\alpha} = 4qi = (q/2)(2+2i)^2$ is a square in $\mathbf{Q}(i)$ implies that $q/2 = r^2$ is the square of some $r \in \mathbf{Q}^*$. Substituting $\alpha = (1 + 2ir^2)^2$ in the model (28), we find that E is \mathbf{Q} -isomorphic to

$$(29) \quad E_r : y^2 = x(x^2 - 2(1 - 4r^4)x + (1 + 4r^4)^2).$$

As we have shown that E_r does have $Z_{E_r/\mathbf{Q}}(2) = Z_{E_r/\mathbf{Q}}(4) = \mathbf{Q}(i)$, this proves the theorem. \square

As the j -invariant $j(E_r)$ of the elliptic curve given by (29) is a non-constant function of r , the family $\{E_r/\mathbf{Q}\}_{r \in \mathbf{Q}^*}$ is non-isotrivial, and represents infinitely many distinct isomorphism classes over $\overline{\mathbf{Q}}$. This yields the following explicit version of Theorem 1.3.

Theorem 5.6. *Let E_r be as above, and K be a number field of degree n . Then all elliptic curves E_r/K with $r \in \mathbf{Q}^*$ have adelic point groups $E_r(\mathbf{A}_K)$ that are not isomorphic to the topological group \mathcal{E}_n .*

Proof. We show that for any $r \in \mathbf{Q}^*$, the torsion closure $T_{E_r/K} = \prod_{\mathfrak{p}} T_{\mathfrak{p}}$ from (10) has 2-rank equal to 0. As $T_{E_r/K}$ is intrinsically defined as the closure of the torsion subgroup of $E_r(\mathbf{A}_K)/E_{r,cc}(\mathbf{A}_K)$, this implies that $E_r(\mathbf{A}_K)$ is not isomorphic to \mathcal{E}_n .

As E_r has by construction a non-complete 2-torsion subgroup $E(\mathbf{R})[2] = \langle(0, 0)\rangle$ over the unique archimedean completion \mathbf{R} of \mathbf{Q} , its discriminant $\Delta(E_r)$ is a negative rational number. By definition (8), we therefore have $T_{\mathfrak{p}} = 1$ for all infinite primes \mathfrak{p} of K .

For \mathfrak{p} a finite prime of K , there are two cases. If $K_{\mathfrak{p}}$ contains i , and therefore $Z_{E_r/K}(4) = K(i)$, the complete 4-torsion of E_r is $K_{\mathfrak{p}}$ -rational, and $E_r(K_{\mathfrak{p}})$ has no direct summand of order 2. In the other case, where $K_{\mathfrak{p}}$ does not contain i , we have $E(K_{\mathfrak{p}})[2] = \langle(0, 0)\rangle$. As all 4-torsion points of E_r are $K_{\mathfrak{p}}(i)$ -rational, we can pick a point $P \in E_r(K_{\mathfrak{p}}(i))$ of order 4 for which $2P$ is a 2-torsion point $T \in E_r(K_{\mathfrak{p}}(i))$ that is not $K_{\mathfrak{p}}$ -rational. Write σ for the non-trivial automorphism of $K_{\mathfrak{p}}(i)$ over $K_{\mathfrak{p}}$. Then the point $Q = P + P^{\sigma} \in E_r[4](K_{\mathfrak{p}}(i))$ is $K_{\mathfrak{p}}$ -rational and

satisfies $2Q = T + T^\sigma = (0, 0)$. It follows that $E(K_{\mathfrak{p}})[4] = \langle Q \rangle \cong \mathbf{Z}/4\mathbf{Z}$ has no direct summand of order 2, and the same is then true for $E(K_{\mathfrak{p}})$. This shows that no $T_{\mathfrak{p}}$ has a direct summand of order 2, and completes the proof. \square

Remark 5.7. It follows from the tables of Rouse and Zureick-Brown [7] that for *all* elliptic curves E/\mathbf{Q} , the inclusion $Z_{E/\mathbf{Q}}(4) \subset Z_{E/\mathbf{Q}}(8)$ is strict, and therefore, by Proposition 5.2, that for such E we have $K_{2^{k+1}} \neq 1$ in (25) for all $k \geq 2$. This implies that for $K = \mathbf{Q}$,

$$\Sigma_{\mathbf{Q}} = \{2\}$$

is the minimal set of prime powers in Theorem 5.4.

Remark 5.8. Both in Lemma 5.1 and in Theorem 5.6, the only value of the ℓ^k -rank of $T_{E/K}$ different from the generic value $e(\ell^k) = \omega$ is $e(\ell^k) = 0$. This is no coincidence, as there is the purely algebraic fact that if a group G acts on a free module M of rank 2 over $\mathbf{Z}/\ell^{k+1}\mathbf{Z}$ in such a way that the module of invariants M^G has a direct summand of order ℓ^k , then there exists an element $g \in G$ such that $M^{\langle g \rangle}$ has a cyclic direct summand of order ℓ^k . Thus, if E/K is an elliptic curve for which $T_{\mathfrak{p}} \subset T_{E/K}$ has a cyclic direct summand of order ℓ^k for a *single* finite prime \mathfrak{p} , then we are in the situation above, with $G \subset G_{\ell^{k+1}}$ the decomposition group of \mathfrak{p} acting on $M = M_{\ell^{k+1}}$ as in (23). It then follows that for the infinitely many primes \mathfrak{p} of K that are unramified in $K \subset Z_{E/K}(\ell^{k+1})$ with Frobenius element in $G_{\ell^{k+1}}$ conjugate to the element $g \in G$ above, $T_{\mathfrak{p}}$ also has a cyclic direct summand of order ℓ^k , leading to the implication

$$e(\ell^k) \neq 0 \implies e(\ell^k) = \omega$$

for the ℓ^k -ranks of $T_{E/K}$. As part of his thesis work, Pagano [5] studies this question in the more general setting of abelian varieties, where he shows that the implication above does hold for sufficiently large ℓ , but not in general.

REFERENCES

- [1] Athanasios Angelakis, *Universal adelic groups for imaginary quadratic number fields and elliptic curves*, Doctoral Thesis, Leiden University & Université Bordeaux, Leiden, 2015.
- [2] Athanasios Angelakis and Peter Stevenhagen, *Imaginary quadratic fields with isomorphic abelian Galois groups*, ANTS X - Proceedings of the Tenth Algorithmic Number Theory Symposium, 2013, pp. 21-39.
- [3] Manjul Bhargava and Arul Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, arXiv:1312.7859 (2013).
- [4] Nathan Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570.
- [5] Carlo Pagano, Doctoral Thesis, Leiden University, Leiden, to appear in 2018.
- [6] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, arXiv:1602.01431 (2016).
- [7] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over \mathbf{Q} and 2-adic images of Galois*, Research in Number Theory **1** (2015), no. 1, 1–34.
- [8] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
- [9] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second Edition, Graduate Texts in Mathematics, vol. 106, Springer, 2009.
- [10] David Zywinia, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), no. 5, 811–826.

DEPARTMENT OF MATHEMATICS, NATIONAL TECHNICAL UNIVERSITY OF ATHENS, 9 IROON POLY-
TEXNEIOU STR., 15780 ZOGRAFOU, ATTIKI, GREECE

MATHEMATISCH INSTITUUT, UNIVERSITEIT LEIDEN, POSTBUS 9512, 2300 RA LEIDEN, THE
NETHERLANDS

E-mail address: `ath.angelakis@gmail.com`

E-mail address: `psh@math.leidenuniv.nl`